第三章

研究方法

本研究希望在AAA架構的環境下，透過以使用者情境為設計依據的存取政策，動態地根據情境來執行身份的驗證、決定資源與服務的存取權，最後再依使用情形進行計費。本章則以第二章所說明的理論為基礎來介紹本研究架構，並說明研究架構之特色、相關元件說明與系統運作流程。

3.1 理論基礎與假設

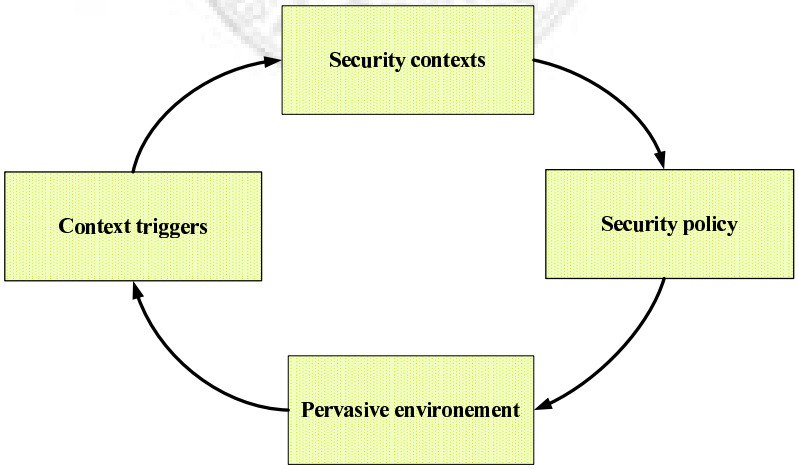

圖 3.1: 情境感知的安全政策概念圖 (Mostéfaoui and Brézillon, 2003)

Mostéfaoui and Brézillon (2003, 2004) 提出以情境為基礎的安全政策 (context-based security policy)，如圖 3.1表示，在普及運算的環境中 (pervasive environment)，系統能夠自動地偵測到環境上的改變，因而造成情境的觸發 (context trigger)；而事先定義好的安全政策 (security policy) 則能夠自動地調整，使其能夠適應新偵測到的安全性情境 (security context)。

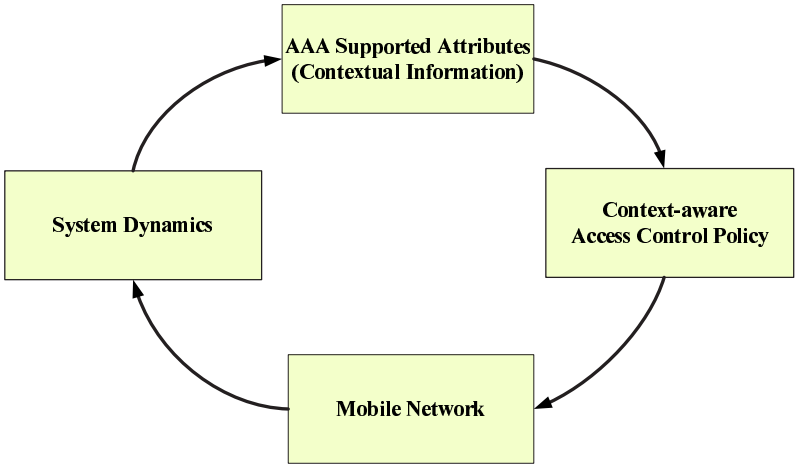

圖 3.2: 概念架構圖

圖 3.2為本系統之概念架構，主要是參考圖 3.1來設計一個整合在 AAA 架構中的安全授權系統。首先假設環境是建置在動態式的行動網路下，最初會受到基本的安全政策所規範。然而環境屬性會隨著時間與移動性的特性發生改變，稱之為系統動態因子 (Schilit, 1995)，在本研究中，這些動態因子也就是所謂的情境。不同型態的情境不斷地發生改變，然而只需針對系統的特殊目的 (例如：身分驗證、授權評估)，蒐集部分會影響到驗證、授權決策或與其他安全政策相關的情境資訊，當這些與安全政策相關的情境發生改變時，系統有能力自動地重新評估授權決策，調整資源存取的設定，使得更能夠根據使用者與環境目前狀態，做出更有彈性且更即時的回應。

3.1.1 行動式網路(mobile network)

行動式的網路環境中，系統會根據最初的情境來決定要依循的安全政策。然而根據圖 3.2所示，動態的環境造成各種情境資訊上的改變，因此驅動不同的存取政策，改變網路環境中對於資源存取的設定、定價的策略等，形成一個持續改變的迴圈。

3.1.2 系統動態因子(system dynamics)

在分散式、可移動式的網路環境中常會存在著許多無法預測的變化，例如：傳輸媒體的不同，會導致不同的頻寬、連線速度等，使得環境是動態而非靜態不變的。當行動工作者在移動時，不僅只是地點上的轉換，傳輸媒體、使用成本與周圍的人物也會產生改變，因此造成不同的情境。系統的動態因子可分為通訊面、環境面與地點面三大面向(Schilit, 1995)：

- 通訊狀態的改變(communication dynamics)

  包括有頻寬、使用成本、安全性的需求程度、通訊時間等。因著這些特性的不同，系統也就必須使用不同的協定、依循不同等級的安全政策或是改變應用系統的運作狀態。

- 環境狀態的改變(environmental dynamics)

  環境狀態主要指的是個人所處的環境資訊，如：周圍的人、實體狀態(燈光、聲音)等。

- 地點的改變(location dynamics)

  行動工作者工作地點的轉移，造成手持設備IP位置、網路拓撲(network topology)的改變，與其他固定設施之間信賴關係的變化等。由於可移動性(mobility)的特性，使用者會隨時地從一個無線

網路的基地台轉移到另外一個基地台的涵蓋範圍(wireless cell)，因此就產生漫遊服務的需求、身分驗證、信賴關係的確認及資源存取權的問題。

3.1.3 驗證、授權與計價相關之屬性(AAA Attributes)

由於環境的動態性，造成使用者情境資訊的改變。根據前面所描述到，環境或系統的動態因子有不同的種類，但是在AAA架構中，則必須蒐集與安全性、存取政策等相關的資訊。安全性的情境資訊是指一組從使用者或應用系統所處的環境中所蒐集到一切與安全政策或是安全防護基礎建設相關的資訊(Mostéfaoui and Brézillon, 2003)。

本研究以AAA-RADIUS伺服器所必須支援有關驗證、授權及計價之屬性(如表3.1)來作為與安全性相關情境資訊的來源基礎。

表 3.1: 驗證、授權及計價之屬性

屬性類別	存取請求	存取回應	計價	附註
User-Name	V	V	V	
User-Password	V			
NAS-IP-Address	V		V	
Service-Type	V	V	V	
Class		V	V	
Framed-Protocol	V	V	V	
Framed-IP-Address	V	V	V	
Called-Station-Id	V		V	
NAS-Identifier	V		V	
Port-Limit		V		
Session-Timeout		V		
Idle-Timeout			V	
Acct-Status-Type			V	
Acct-Delay-Time			V	
Acct-Session-Id	V		V	
Acct-Authentic			V	
Event-Timestamp			V	
Acct-Input-Gigawords			V	
Acct-Output-Gigawords			V	

資料來源：RADIUS 伺服器支援之屬性

除了上述所描述的屬性外，在安全性的情境資訊中，還必需包含通訊狀態、遠端資源的可得性、存取時間、使用者的安全等級與其目前的執行環境

3.1.4 情境感知的存取政策(context-aware access control policy)

系統管理者或服務提供者不能夠事先知道所有可能存取者的身分帳號與密碼，因此無法完整且明確地定義出每一項資源的所有存取名單。在本研究中，我們則以情境來作為存取政策的設計考量。因此，只要當所蒐集到的情境滿足身份驗證與存取條件的設定時，就會驅動適合的存取政策，允許資源或服務的使用。

當行動工作者移動其工作地點或外在其他環境因素變動時，個人情境資訊也會相對地發生改變。此時系統會要求重新驗証使用者的身分，並根據改變後的情境執行不同的授權或資源、服務的存取，驅動不同的計價策略。

3.2 系統特性

AAA 架構與相關協定主要是希望能夠解決在分散式、異質的環境中有關認證、授權與計價之問題。透過存取控制的機制，最終目的要能滿足系統的安全性需求，限制使用者的操作與活動。然而由於行動式網路環境多變的特性，在驗證與授權等問題上，不能僅以傳統的靜態的資料或唯一的屬性來做考量。因此在設計授權政策或是存取控制政策時，還必需加上各種情境、使用者或是手持設備定義檔等資訊，使得系統能夠根據目前執行環境有效地調整安全政策，達到有效的安全防護機制。以下即描述以此概念為設計基礎的AAA 架構之特點：

1. 行動式的運作環境

   結合各種無線上網技術與無線網路的存取服務，AAA 架構是在一個行動式的網路環境中運作的。使用者(行動用戶)也因此具備可移動性的特性。

2. 環境敏感性

   由於整個執行背景是建立在移動式網路下，環境中的各項變數都會直接或間接影響到行動用戶與網路服務業者之間的通訊過程。通訊狀態會因為環境的不同而改變，而系統的安全政策也因著這些變數作調整，改變授權決策，達到即時的調整與配置(run-time configuration)，使其具備著時間敏感性(time-sensitive)、地點敏感性(location-sensitive) 等。

3. 自發性

透過前端感應器(sensor)、監控器(monitor)與後端以情境為設計基礎的存取控制政策結合，能夠自動地偵測情境的改變，依情境之不同，自發性地驅動適當的存取政策，動態且即時地調整服務存取決定。

4. 適切性

能夠根據目前的執行環境、地理位置、使用者特性、安全等級等變數，即時地評估授權決策，以提供適切與適地的網路存取服務，滿足個人與系統雙方安全性之需求。

3.3 系統架構

根據上述理論與基礎，本研究擬發展一個建立在跨網域AAA架構(Inter-domain AAA Architecture)中的情境感知的系統，除了情境的感知技術與處理以外，並強調並以情境來作為資源存取政策的設計原則，希望能透過一個彈性設計的情境感知安全政策，來解決無線網路環境中資源存取的複雜性。另外，還能利用多樣化的情境資訊來滿足傳統存取控制中僅使用帳號與密碼來進行身分驗證之不足。

圖3.3為本系統主要的執行場景。在跨網路的無線網路環境中，會有多個子網域存在，其中包含一個使用者本身所註冊的主網域(home domain)與其它漫遊網域(visted domain, romaing domain)。當使用者欲存取網路資源時，系統會先確認其網路位置是否在主網域內。一旦網路位置離開主網域的範圍時，使用者必須先向其他的網路服務業者(Visted ISP)申請漫遊的服務，此時兩個不同的網路間便會開始進行一連串的驗證與授權程序，並根據主網域和漫遊網域之間的協定，來決定是否有網路的存取權。

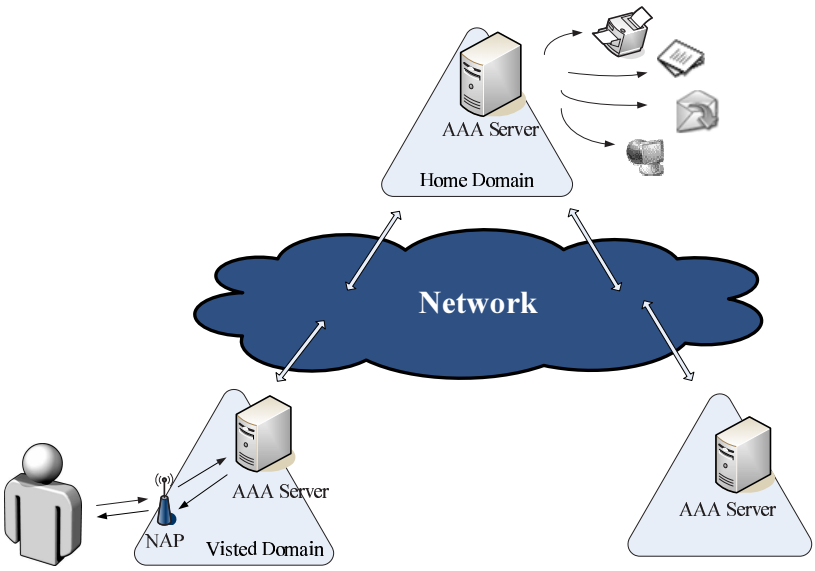

圖 3.3: 跨網域環境

不論是在主網域或是漫遊網域中，都是建立在AAA 架構下，因此會包含一個執行驗證、授權與計費服務的AAA 伺服器與其他元件。而在本研究所發展的系統(圖：3.4)雛型中，除了上述AAA 架構中的基本元件，另外設計出情境偵測服務及情境處理器。透過這些情境感知的應用系統，可以有效地偵測、解釋、管理、使用行動用戶的情境資訊，最後針對情境做出適當地回應，提供合適的服務，滿足之前所描述的系統特性。

3.4 架構元件

在本節中會介紹用來處理情境的相關元件。因此在完整的AAA 架構環境下，透過各元件間的協調與合作，彈性且即時地回應行動用戶服務請求、保障無線網路安全。

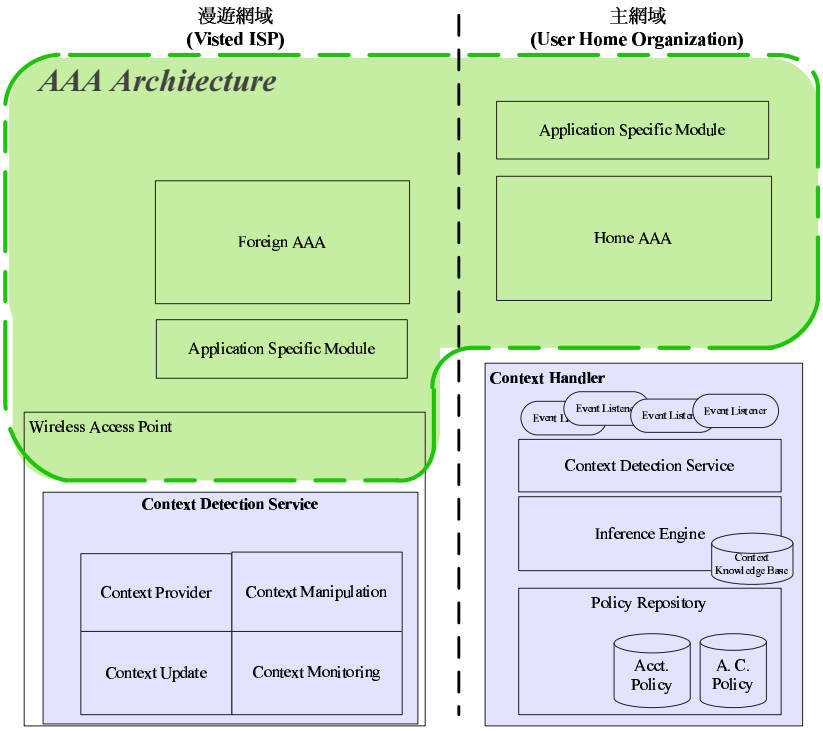

圖 3.4: 建構在 AAA 架構下的情境感知授權系統

3.4.1 情境偵測服務

情境偵測服務 (context detection service) 主要目的是用來偵測 (detect)、識別 (identify) 所有的行動用戶與資源，蒐集使用者的情境。最後還要能有效地進行情境的管理與監督。情境偵測服務 (圖 3.5包含下列四個子元件：

情境提供 **(Context Provider)**

透過感應器或其他第三方伺服器等來取得有關行動用戶的情境資訊。例如：利用 GSM、GPRS 等服務，取得有關使用者的地理資訊；藉由偵測軟體，感應使用者目前的作業環境等。在本系統中，為了滿足存取政策資訊上的需求，必須蒐集有關行動用戶與資源 (服務) 的情境：

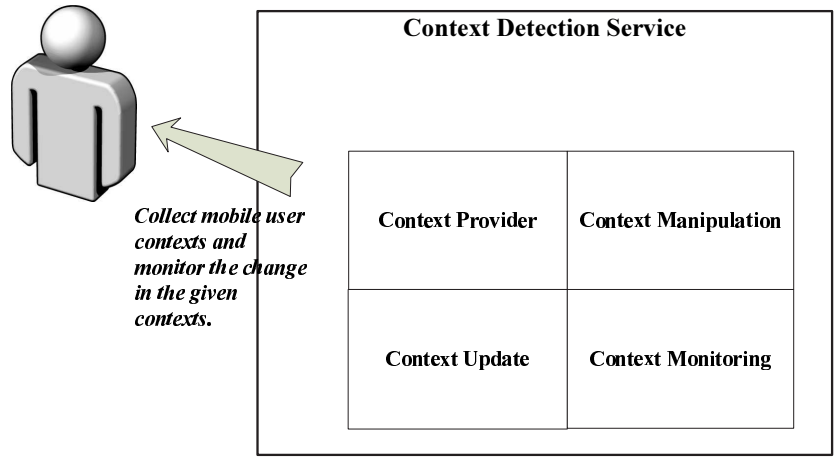

圖 3.5: 情境偵測服務

1. 行動用戶

   當行動用戶開始與無線網路存取點進行對話時，便開始進行身分上的識別，主要提供的資訊有：

   - 時間。
   - 目前實際地理位置與行動設備IP位址。
   - 驗證、授權與計價政策中所要求的資訊。
   - 網路的通訊狀態。
   - 同一區域內其他行動用戶的相關訊息。
   - 行動用戶或行動設備目前的作業環境。

2. 所提供的資源(服務)

   負責處理在本地端資源情境的偵測(如:使用狀態)，主要提供的資訊包含：

   - 資源的可得性(availability)。

- 目前資源的使用狀態(正在存取的人數等)。
- 資源所要求的安全等級。
- 資源所在地點及其他特性。

上述所偵測到的情境，屬於第一級資訊。第一級資訊並沒有使用共通的表達方式，但為了滿足網路環境中分散式伺服器的需求，因此必需再經過處理與抽象化，形成以本體論做為表達方式的標準情境物件(ontology-based context)，屬於第二級資訊。這類型的情境物件會連同行動用戶所提供的個人身分資訊(帳號/密碼)、請求的服務類別(service type)等形成存取請求訊息(access request message)送到目前網路存取點所屬的AAA伺服器(Foreign AAA)，請求驗證與授權。

情境操作**(context manipulation)**

情境操作的目的是根據一個正式的情境模型(context model)中所建立的類別層級與關係，來描述環境中的情境資訊。因此透過進一步的情境操作以提供正式、標準的情境資訊，這也就是之前所描述的第二級情境資訊。本研究以本體論(ontology)的方式為模型建置基礎，並根據系統的特殊目的，如：存取控制，來設計不同的情境類別、屬性與情境間的關係等。在第四章中，將會詳細地介紹針對存取控制政策所設計的情境模型。

因此在情境發現、偵測與蒐集後，系統會根據已定義好的情境模型，以OWL(ontology web language)[1]來描述環境中的情境資訊與屬性。使得情境能夠以標準的方式來做呈現，同時滿足在分散式環境下的互通性(interoperability)、語義表達(semantic representation)與邏輯推論(logic reasoning)之需求。

[1]http://www.w3.org/2004/OWL/

圖:3.6為本研究所定義有關行動用戶之部分語義。行動用戶主要是本授權系統的授權對象，因著系統的需求，並需定義出使用者的所在位置和其欲從事的行為等。

```
<owl:Class rdf:ID="#User">
  <rdfs:subClassOf>
      <owl:Restriction>
        <owl:onProperty rdf:resource="#located in"/>
      </owl:Restriction>
  </rdfs:subClassOf>
  <rdfs:subClassOf>
     <owl:Restriction>
         <owl:onProperty rdf:resource="#engaged in"/>
      </owl:Restriction>
  </rdfs:subClassOf>
</owl:Class>
```

圖 3.6: 行動用戶 ontology 範例

情境監控 **(context monitoring)**

當行動用戶通過身分驗證後，便開始進行漫遊服務，存取網路與其他資源等。在整個對話與資料通訊的過程中，有關通訊面、環境面或地點面的環境動態因子會隨時地發生改變，因此必須透過情境監控元件負責監控最初的情境資訊是否發生改變。

情境更新 **(context update)**

一旦情境發生變動後，情境更新服務就會被啟動。根據所蒐集到最新的資訊，修改使用者暫存區中的資料，並依一定的時間間隔(雙方所約定的資料傳遞頻率)，將更新後的情境傳送給AAA伺服器。

Foreign AAA 則負責轉送這些資訊給適合的 Home AAA，請求身分的再次驗證。

在 AAA 伺服器上會有特定的事件監聽器來負責特定行動用戶的對話當接收到有關行動用戶情境改變的事件後，過去的資源存取條件不再被滿足，不同的授權政策或計價策略開始被驅動，整體的安全政策也因此跟著調整。最後根據最新的驗證評估結果，來決定是否要繼續允許資源的存取或是撤銷過去所給予的許可權，拒絕使用者的存取。

3.4.2 情境處理器

情境處理器 (context handler) 主要是設置在 Home AAA 的一項元件，負責處理在本地端情境的偵測 (如 : 資源的使用狀態)、推論與、情境更新各種有關存取控制政策的儲存與管理。情境處理器 (圖 refctx2) 功能介紹如下：

事件監聽器

當行動用戶開始與 AAA 伺服器進行對話與存取服務時，系統會自動地針對每一個連線中的用戶，來註冊屬於個人的事件監聽器 (event listener)，用來負責處理事件的內容。在整個對話期間，當 AAA 伺服器接收到用戶情境改變的訊息時，會直接把這個改變的情境資訊，也就是事件來源 (event source)，傳遞給特定的事件監聽器，執行其它後續動作。

推論引擎

為了要能根據行動用戶的情境來決定資源的存取權限，本系統採用規則式的推論引擎 (rule-based inference engine)，來推導出合適的安全授權政策。因此利用不同的推論能力，使得系統可以從外顯 (explicit) 的

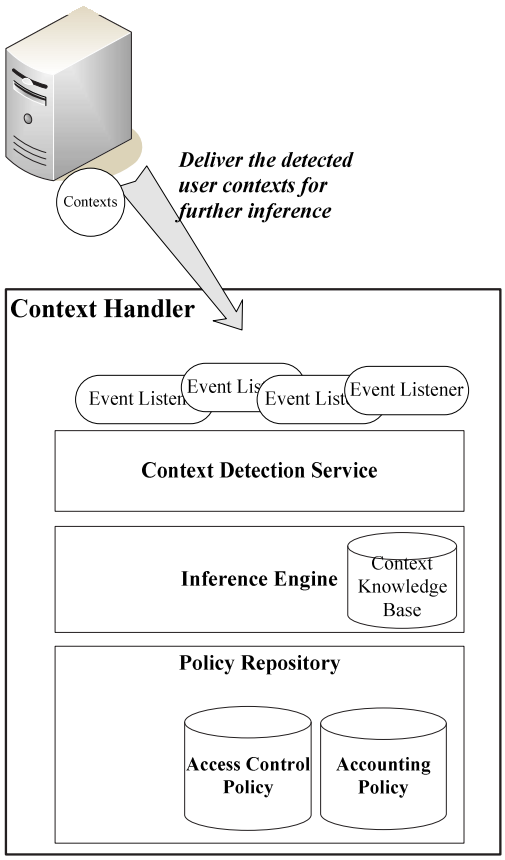

圖 3.7: 情境處理器

情境來引導出無法從感應器偵測到的內隱 (implicit) 情境，藉以滿足推論之豐富性。另外也能透過適當的推論機制，來維持情境資料庫之一致性、解決各種衝突的情況發生。

在本系統的論論引擎中，主要分為兩種推論能力：

表 3.2: 本體論中的推論規則

推論規則	描述
subClassOf	類別之間的繼承關係
subPropertyOf	屬性之間的繼承關係
inverseOf	反屬性關係
TransitiveProperty	屬性間的遞移性
SymmetricProperty	屬性間的對稱性

參考自 W3C: OWL Web Ontology Overview

1. 本體論中所衍生出的語義規則 (Ontology reasoning rules)

   透過ontolgy內建的語義規則，可以表達基本的類別之間的關係、屬性間的關係或基數 (cardinality) 上的限制等。因此推論引擎可以根據這些規則做初步的推論。因此在設計存取控制政策時，可以利用這些內間的關係表達實際情境類別間的關連。表3.2為參考W3C所定義的本體論所整理出的推論規則。例如經理 (Manager) 與行動用戶 (User) 兩類別間存在著繼承 (owl:subClassOf) 的關係，因此一個經理的實體 (instance) 同樣也會是行動用戶的實體。

2. 使用者定義的推論規則 (User-defined reasoning rules)

   前面描述的是較基本的語義規則；若需要表現更複雜的語義關係，則必需自行定義出系統所需要的推論規則。因此管理人員根據使用者情境、網路需求或是系統安全等級等推論出不同的安全政策或資源存取上之限制，就是一個彈性的推論規則的表現。表3.4.2為本研究所設計的部份推論規則。

表 3.3: 存取控制政策之推論規則

推論規則		推論結果
if (加密需求為高強度加密) 且 (使用 L2TP/IPSec VPN 連線方式)	⇒	使用 3DES 加密
if (代理伺服器位置為 proxy.nccu 且 (使用區域網路的連線方式)	⇒	允許使用網路印表機
if (連線位置非區域網路) 且 (存取目標為電子郵件系統)	⇒	允許使用信箱 限制連線時間為 25 分鐘

情境資料庫

用來儲存系統所使用的情境資訊，提供基本的新增、修改、刪除與查詢的功能。

存取政策

建立在使用者原始註冊的網域內之 AAA 伺服器，主要是負責執行驗證身份、決定授權決策與服務收費。在本系統中，主要是建立一個有關網路資源存取的安全授權系統，使得 AAA 伺服器可以透過情境處理器 (CH) 中的政策儲存體 (policy repository) 來儲存已定義好的存取政策，並再根據已定義授權存取政策與內建的推論系統，來決定所應要執行的安全措施。

本系統所設計的存取政策 (圖：3.8) 由三大部分所組成：目標 (target)、評估許可 (effect)、個人設定 (configuration))。當存取政策中的條件全部被滿足時，系統會授予使用者資源存取權，並針對不同的行動用戶建立特殊的連線設定。詳細內容會在第四章-存取政策設計中作介紹。

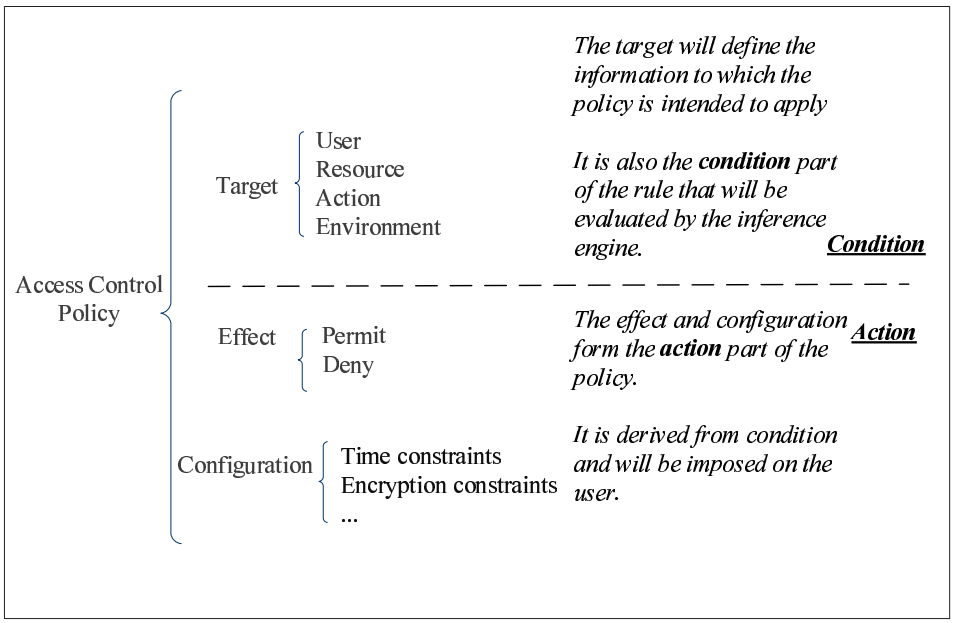

圖 3.8: 存取控制政策之設計概念

3.5 運作流程

結合上述所說明的元件與基本的AAA架構，本研究架構則如圖 3.9所示，情境感知的安全系統與AAA伺服器等元件間的運作流程如下：

1. 行動用戶向無線網路存取點要求存取網路服務。
2. 當無線存取點接收到使用者的請求後，
   2.1. 情境偵測服務(context detection service)會透過感應器(sensor)來感應有關使用者的情境(context)。
   2.2. 將行動用戶的情境(存取時間、地點、網域等)、驗證資訊與網路存取識別碼(Network Access Identifier, NAI)傳遞給漫遊端AAA伺服器(Foreign AAA)。

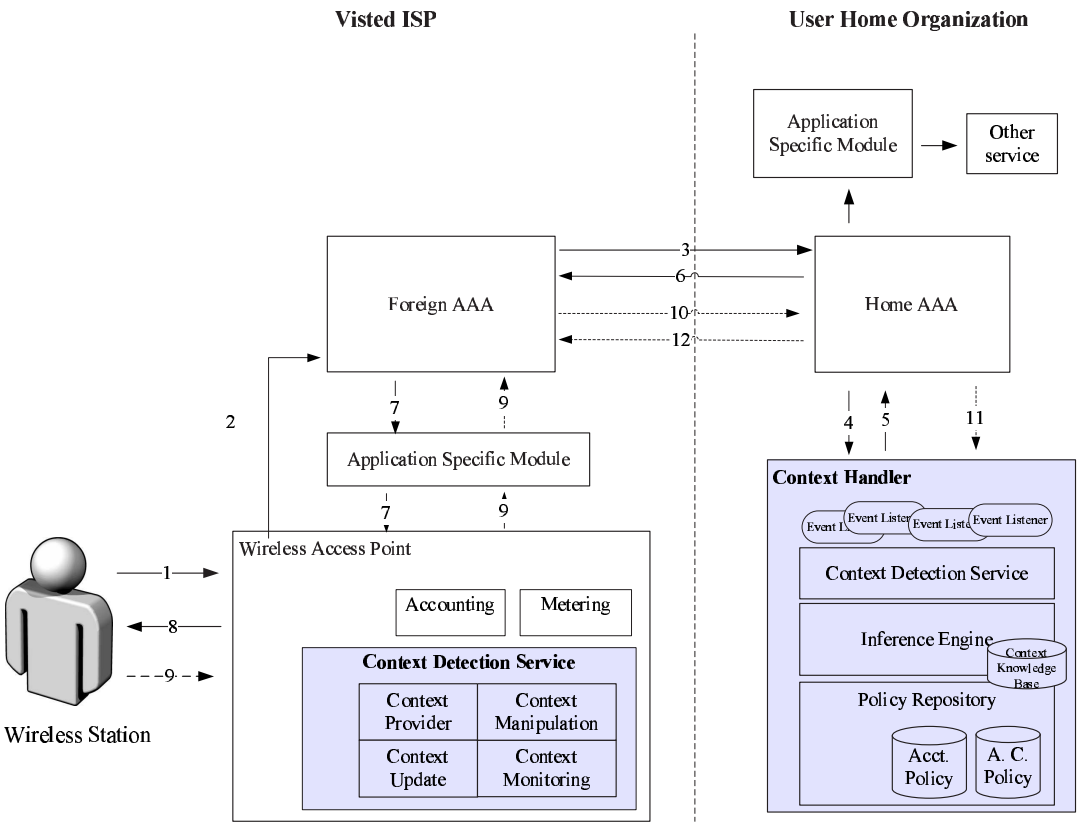

圖 3.9: 系統架構圖

3. Foreign AAA 會根據NAI，將驗證資訊傳遞給正確的本端AAA伺服器 (Home AAA)。

4. 使用者註冊端之AAA伺服器 (Home AAA) 則再將使用者的情境資訊傳遞給情境處理器 (Context Handler, CH)。

5. CH 中的推論引擎 (inference engine) 則根據所接收到的情境，驅動不同的存取政策。

6. Home AAA 將評估後的結果 (接受 / 拒絕請求) 與相關的設定資訊 (service configuration) 傳回Foreign AAA

7. Froeign AAA 根據評估後的結果來接受或拒絕使用者的請求 (access accept/access reject)，並透過特殊應用系統模組 (Application Specific Module, ASM) 來設定與使用者相關的服務參數。

8. 無線存取點則通知行動用戶最後的評估結果。一旦通過身分驗證後，便可開始進行資料傳輸等漫遊的服務。

9. 在連線的過程中，CDS 會持續負責監視使用者情境上的變動。

10. 一旦情境改變時，例如：連線方式由 WLAN 轉換至 3G 傳輸，Foreign AAA 會依約定的更新頻率將改變後的情境傳送給 Home AAA，請求身分的再次驗證並決定是否能夠繼續存取該資源服務。

11. 透過事件監聽器 (event listener) 負責接收情境變動的事件，並重新再驅動不同的授權政策，評估資源存取決策。

12. Home AAA 將改變後個人連線設定傳回給 Foreign AAA，因此系統可以根據新偵測到的情境，重新調整系統安全政策以適應新的環境。

另外 AAA 伺服器則會再針對不同行動用戶的使用情形，進行服務的計費與收費 (accounting) 等操作，則不在本研究範圍內。